

I hereby certify that this correspondence is being filed via
EFS-Web with the United States Patent and Trademark Office
on September 15, 2009

PATENT
Attorney Docket No. 026595-007510US

TOWNSEND and TOWNSEND and CREW LLP

By: /Dianna L. Smith/
Dianna L. Smith

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

John M. Morales et al.

Application No.: 10/658,844

Filed: September 8, 2003

For: SYSTEMS AND METHODS FOR
PRODUCING SUSPICIOUS ACTIVITY
REPORTS IN FINANCIAL
TRANSACTIONS

Confirmation No. 5408

Examiner: Clement B. Graham

Technology Center/Art Unit: 3696

**APPELLANTS' BRIEF UNDER
37 CFR §41.37**

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Further to the Notice of Appeal mailed on July 15, 2009, for the above-referenced application, Appellants submit this Brief on Appeal.

1. Real Party In Interest

The Western Union Company, of Englewood, Colorado, is the real party in interest as the assignee of the above-identified application.

2. Related Appeals And Interferences

No other appeals or interferences are known that will directly affect, are directly affected by, or have a bearing on the Board decision in this appeal.

3. Status Of Claims

Claims 1-5, 11-14, 16, and 18-22 are currently pending in the application. All pending claims stand finally rejected pursuant to a final Office Action mailed January 23, 2009 ("Final Office Action"). A copy of the claims as rejected is attached hereto in the Claims Appendix.

Claims 1-5, 11-14, 16, and 18-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0024693 to Lawrence ("Lawrence") in view of U.S. Patent Publication No. 2004/0006532 to Lawrence et al. ("Lawrence1"). **This rejection is the subject of the appeal.**

Claims 6-10, 15, and 17 were previously canceled.

4. Status Of Amendments

No amendments have been entered subsequent to the Final Office Action.

5. Summary Of Claimed Subject Matter

In the following summary, the Appellants have provided exemplary references to sections of the specification and drawings supporting the subject matter defined in the claims as required by 37 C.F.R. § 41.37. The specification and drawings also include additional support for other exemplary embodiments encompassed by the claimed subject matter. Thus, it should be appreciated that the references are intended to be illustrative in nature only.

In the embodiment of claim 1, a method of producing a suspicious activity report is described. *Application*, p. 2, l. 28 – p. 3, l. 1. The method includes storing configuration information at a transaction processing device. *Id.*, at p. 3, ll. 1, 2. The configuration information configures the device to produce suspicious activity reports based on certain criteria. *Id.*, at p. 3, ll. 2, 3. Further, the certain criteria comprise both a mandatory SAR threshold and a SAR prompt threshold. *Id.*, at p. 8, ll. 25, 26; p. 8, l. 30 – p. 9, l. 1. The method also includes receiving transaction information. *Id.*, at p. 3, ll. 3, 4. The method further includes determining, based on the transaction information and the certain criteria, whether a suspicious activity report

is to be prepared. *Id.*, at p. 3, ll. 4, 5. Wherein determining whether a suspicious activity report is to be prepared comprises: comparing an amount of a transaction to the mandatory SAR threshold (*Id.*, at p. 9, ll. 29, 30) and, in accordance with the comparison, generating a suspicious activity report containing at least some of the transaction information (*Id.*, at p. 3, ll. 5, 6); and comparing an amount of a transaction to the SAR prompt threshold (*Id.*, at p. 3, ll. 17, 18) and, in accordance with the comparison, displaying a prompt that asks an operator if he wants to prepare a suspicious activity report. *Id.*, at p. 3, ll. 17-21.

In the embodiment of claim 5, a method of producing a suspicious activity report is described. *Id.*, at p. 2, l. 30 – p. 3, l. 1. The method includes storing configuration information at a transaction processing device. *Id.*, at p. 3, ll. 1, 2. The configuration information configures the device to produce suspicious activity reports based on certain criteria. *Id.*, at p. 3, ll. 2, 3. The method includes receiving transaction information. *Id.*, at p. 3, ll. 3, 4. The method also includes determining, based on the transaction information and the certain criteria, whether a suspicious activity report is to be prepared. *Id.*, at p. 3, ll. 4, 5. The method further includes generating a suspicious activity report containing at least some of the transaction information. *Id.*, at p. 3, ll. 5, 6. Generating a suspicious activity report comprises: printing a suspicious activity report having a portion of the additional information (*Id.*, at p. 3, ll. 12-14) and also having blanks for receiving additional suspicious activity report information. *Id.*, at p. 3, ll. 14, 15.

In the embodiment of claim 14, a transaction processing device is described. *Id.*, at p. 3, ll. 26-28. The device includes an input device arranged to receive transaction information and SAR information. *Id.*, at p. 3, ll. 27, 28. The device also includes a display screen arranged to display information to an operator. *Id.*, at p. 3, l. 28. Also included is application software that programs the transaction device to: store configuration information (*Id.*, at p. 3, l. 29), wherein the configuration information configures the device to produce suspicious activity reports based on certain criteria (*Id.*, at p. 3, ll. 28-30), wherein the certain criteria comprise both a SAR prompt threshold and a mandatory SAR threshold (*Id.*, at p. 8, l. 25, 26; p. 8, l. 30 – p. 9, l. 1); receive transaction information (*Id.*, at p. 3, l. 30 – p. 4, l. 1); determine, based on the

transaction information and the certain criteria, whether a suspicious activity report is to be prepared (*Id.*, at p. 4, ll. 1, 2); and generate a suspicious activity report containing at least some of the transaction information. *Id.*, at p. 4, ll. 2, 3.

6. Grounds Of Rejection To Be Reviewed On Appeal

Issue 1: Whether claims 1-5, 11-14, 16, and 18-22 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Lawrence in view of Lawrence1.

7. Argument

Issue 1: Whether claims 1-5, 11-14, 16, and 18-22 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Lawrence in view of Lawrence1.

Claims 1-5, 11-14, 16, and 18-22 stand rejected under various §103 rejections. To support a rejection under 35 U.S.C. §103, the Office is charged with demonstrating that all limitations of the claims are taught or suggested by the prior art (MPEP § 2142) and with “identify[ing] a reason that would have prompted a person of ordinary skill in the relevant field to combine the [prior art] elements” in the manner claimed. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007). In this instance, at least some of the limitations for which the Office relies on Lawrence are not in fact disclosed in that reference.

Claim 1 recites: “storing configuration information at a transaction processing device, wherein the configuration information configures the device to produce suspicious activity reports based on certain criteria, and wherein the certain criteria comprises both a *mandatory SAR threshold* and a *SAR prompt threshold*” Emphasis added. Independent claim 14 contains similar recitations. The Final Office Action maintains that such recitations are taught, suggested, or otherwise proved obvious by Lawrence. Appellant disagrees.

The above recitations from claim 1 include a “mandatory SAR threshold” and a “SAR prompt threshold.” When a “mandatory SAR threshold” is triggered, a SAR (Suspicious Activity Report) is initiated automatically. When a “SAR prompt threshold” is triggered, a SAR may be initiated at a user’s discretion. For example, with a “SAR prompt threshold,” an operator

may be prompted "Produce SAR?" At such a time, the user may then elect to initiate a SAR or proceed without a SAR being generated.

The Office maintains that both a "mandatory SAR threshold" and a "SAR prompt threshold" are taught, suggested, or otherwise proved obvious by Lawrence. *Final Office Action*, p. 7. In allegedly teaching these thresholds, the Office apparently relies upon the "risk criteria" of Lawrence. *Id.* However, Lawrence's "risk criteria" are insufficient to teach, suggest, or otherwise prove obvious both thresholds.

According to Lawrence, "Data received may be structured according to risk criteria and utilized to calculate a risk quotient 108." *Lawrence*, ¶67. This "Risk Quotient 108 can be calculated by multiplying a weighted numerical value of the specific information times the category weighting." *Id.*, at ¶78. Lawrence then discloses that the Risk Quotient may be a score calculated from a variety of variables representing weighted risk scores. *Id.*, at ¶¶ 78, 79. Using this calculated score, risk clearing is accomplished:

Risk clearing that is part of a normal course of business, may simply look for a risk quotient 108 or other risk rating to be below a threshold. Depending upon a level of risk calculated as well as the reasons for the risk calculation, at 316, a responsive action 114 can be generated that is commensurate with the level of risk and the underlying reasons.

As an example, in response to a high risk score, a responsive action 114 may recommend that a Financial Institution not proceed with a transaction, or that an appropriate authority be notified. In response to a low risk score, the Financial Institution may respond by completing a transaction as usual. Intermediate scores may respond by suggesting that additional information be gathered, that transactions for this account be monitored or other interim measures.

Id., at ¶¶80, 81, emphasis added. While Lawrence focuses on various risk scores resulting in transactions being treated differently, Lawrence clearly does not teach, suggest, or otherwise disclose: a *mandatory* SAR threshold *and* a SAR *prompt* threshold. Rather, Lawrence uses the "Risk Quotient" to produce *suggested* or *recommended* courses of actions. Lawrence does not consider the possibility of a device configured to have a *mandatory* suspicious activity report generated at a threshold *and* having a threshold where a suspicious activity report is *prompted* for, but not required.

For at least these reasons, claims 1 and 14 are not taught, suggested, or otherwise proved obvious by the cited references. Therefore, a *prima facie* case of obviousness was properly not established. Accordingly, Appellant respectfully requests reversal of the §103 rejections of claims 1 and 14. Further, claims 2-4, 11-13, 16, and 18-22 depend, either directly or indirectly, from claims 1 and 14. At least by virtue of their dependence on claims 1 and 14, a *prima facie* case of obviousness has likewise not been properly established for claims 2-4, 11-13, 16, and 18-22. Appellant respectfully requests reversal of the §103 rejection.

With regard to claim 5, claim 5 recites: "wherein generating a suspicious activity report comprises: printing a suspicious activity report having a portion of the additional information and also having blanks for receiving additional suspicious activity report information." Such recitations are not taught, suggested, or otherwise proved obvious by the cited reference.

To allegedly teach, suggest, or otherwise prove obvious such recitations, the Final Office Action cites to Lawrence paragraphs 89 and 91. In its entirety, the cited portion of Lawrence recites:

At 417, a user can also cause an archive to be created relating to Risk management. An archive may include, for example, information received relating to Risk associated with a Financial Transaction, as well as steps taken to address the Risk, and a Risk Quotient. In addition, at 418, the user can cause a PRM server 211 to generate reports that can include, for example, a description of related informational data and informational artifacts and otherwise document actions taken to address due diligence relating to Risk management.

....

Referring now to FIG. 6, an exemplary GUI for presenting reports or suggested actions related to PRM is illustrated 600. The GUI for presenting reports 600 can include geographic areas of a user interface containing risk management procedures 601, including those procedures specifically followed in relation to a particular PRM query or other suggested actions. Additional areas can include a list of electronic or hardcopy reports available concerning risk management efforts undertaken 602. Another area can include a list of risk quotients and/or calculations concerning a risk quotient, such as the average risk quotient for the financial institution, or the mean risk quotient 603. Still another

area can contain information descriptive of a particular transactor or other FRM risk subject 604.

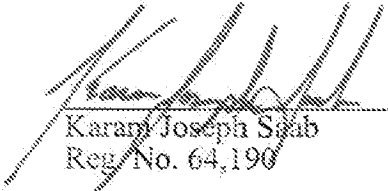
Lawrence, ¶¶89, 91. The Office provides no justification how these recitations show 1) printing 2) of a suspicious activity report, and 3) having blanks for additional suspicious activity report information. While the reference discusses storing the Risk Quotient, this is not the same as storing a SAR. Apart from the storing and documenting of the Risk Quotient, it is unclear how the cited portions of the reference, or the reference as a whole, may be interpreted as teaching, suggesting, or otherwise proving obvious such recitations of claim 5.

For at least these reasons, claim 5 is not taught, suggested, or otherwise proved obvious by the cited references. Therefore, a *prima facie* case of obviousness was not established. Accordingly, Appellant respectfully requests reversal of the §103 rejections of claim 5.

8. Conclusion

For these reasons, it is respectfully submitted that the rejection should be reversed.

Respectfully submitted,



Karan Joseph Seab
Reg. No. 64,190

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 303-571-4321

62207932 v1

9. Claims Appendix

1. (Previously Presented) A method of producing a suspicious activity report, comprising:

storing configuration information at a transaction processing device, wherein the configuration information configures the device to produce suspicious activity reports based on certain criteria, and wherein the certain criteria comprises both a mandatory SAR threshold and a SAR prompt threshold;

receiving transaction information;

determining, based on the transaction information and the certain criteria, whether a suspicious activity report is to be prepared, wherein determining whether a suspicious activity report is to be prepared comprises:

comparing an amount of a transaction to the mandatory SAR threshold and, in accordance with the comparison, generating a suspicious activity report containing at least some of the transaction information; and

comparing an amount of a transaction to the SAR prompt threshold and, in accordance with the comparison, displaying a prompt that asks an operator if he wants to prepare a suspicious activity report.

2. (Original) The method of claim 1, further comprising transmitting the suspicious activity report to authorities.

3. (Original) The method of claim 2, wherein transmitting the suspicious activity report to authorities comprises:

collecting suspicious activity reports at a host computer system; and

transmitting the collected suspicious activity reports to a computer system of the authorities.

4. (Original) The method of claim 1, further comprising receiving additional information and including the additional information in the suspicious activity report.

5. (Previously Presented) A method of producing a suspicious activity report, comprising:

storing configuration information at a transaction processing device, wherein the configuration information configures the device to produce suspicious activity reports based on certain criteria;

receiving transaction information;

determining, based on the transaction information and the certain criteria, whether a suspicious activity report is to be prepared; and

generating a suspicious activity report containing at least some of the transaction information;

wherein generating a suspicious activity report comprises:

printing a suspicious activity report having a portion of the additional information and also having blanks for receiving additional suspicious activity report information.

6. – 10. (Canceled)

11. (Original) The method of claim 1, wherein determining whether a suspicious activity report is to be prepared comprises determining whether an operator has elected to produce an on-demand SAR.

12. (Original) The method of claim 1, further comprising printing a report relating to suspicious activity reports produced at the transaction processing device during a period of time.

13. (Original) The method of claim 1, wherein the transaction processing device is configured to print money orders.

14. (Previously Presented) A transaction processing device, comprising:
an input device arranged to receive transaction information and SAR information;
a display screen arranged to display information to an operator; and

application software that programs the transaction device to:
store configuration information, wherein the configuration information configures the device to produce suspicious activity reports based on certain criteria, wherein the certain criteria comprises both a SAR prompt threshold and a mandatory SAR threshold;
receive transaction information;
determine based on the transaction information and the certain criteria, whether a suspicious activity report is to be prepared; and
generate a suspicious activity report containing at least some of the transaction information.

15. (Canceled)

16. (Previously Presented) The transaction processing device of claim 14, wherein the application software also programs the transaction device to compare an amount of a transaction to the mandatory SAR threshold.

17. (Canceled)

18. (Previously Presented) The transaction processing device of claim 14, wherein the application software also programs the transaction device to compare an amount of a transaction to the SAR prompt threshold.

19. (Original) The transaction processing device of claim 18, wherein the application software further programs the transaction device to:
display a prompt that asks an operator if he wants to prepare a suspicious activity report; and
receive a response to the prompt.

20. (Original) The transaction processing device of claim 14, wherein the application software also programs the transaction device to determine whether an operator has elected to produce an on-demand SAR.

21. (Original) The transaction processing device of claim 14, wherein the application software further programs the transaction device to print a report relating to SARs produced at the transaction processing device during a period of time.

22. (Original) The transaction processing device of claim 14, wherein the transaction processing device is configured to print money orders.

10. Evidence Appendix

No additional evidence is provided.

11. Related Proceedings Appendix

No additional proceedings are in process.